Remarks

1. Status of the Claims

Claims 1, 3-9, 11-17, and 19-21 are pending. Claims 2, 10, and 18 are cancelled herein. Claims 1, 3, 4, 9, 11, 16, and 21 are presently amended. The Examiner stated that claims 6-7, 13, and 15 are objected to as being dependent upon rejected base claims but would be allowable if rewritten in independent form. The Examiner has also objected to claim 9 due to lack of antecedent basis. The Examiner rejected claims 1-3, 5, 8-12, 14, and 16-21 under 35 U.S.C. § 103(a) as being obvious over Applicants' allegedly Admitted Prior Art (AAPA) in view of U.S. Patent No. 6,965,994 to Brownell et al (Brownell). The Examiner has also rejected claim 4 under U.S.C. § 103(a) as being obvious over AAPA in view of Brownell, further in view of U.S. Patent Pub. No. 20040006700 to Freeman et al.

2. Objections to the Claims

Applicants respectfully acknowledge the Examiner's statements that claims 6-7, 13, and 15 would be allowable if rewritten in independent form. Additionally, Applicants have corrected the lack of antecedent basis in independent claim 9. Applicants respectfully request that the objection to this claim be withdrawn.

3. Independent Claims 1, 9, 16, and 21

The Examiner has rejected independent claims 1, 9, 16, and 21 as being obvious over the combination of AAPA and Brownell. To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). If an independent claim is nonobvious under 35 U.S.C. 103, then any

claim depending therefrom is nonobvious. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Because the above-cited combination fails to teach or suggest each and every claim limitation of the independent claims, a *prima facie* case of obviousness has not been established. Specifically, the Examiner has not shown that the combination of AAPA and Brownell teaches or suggests that the step of verifying that the firmware update application has the authority to perform the firmware update comprises the step of determining whether the firmware update application has access to a **predetermined encryption key utilized by the computer system.**

In the present invention, once a user initiates a firmware update application, the BIOS of the computer system generates a random token (T), which is encrypted (as seen in step 52 of Figure 3) with a predetermined key. This same token (T) is passed to the firmware update application, which then encrypts the token with its own encryption key and provides the result to the BIOS. The BIOS performs a comparison step (58) to see whether the results of the two encryptions of the token match. If the results match, the firmware update process is determined to have access to the predetermined encryption key utilized by the computer system (in this case, the BIOS) and further verification may proceed, such as user verification. (Spec., p.7, line 17-p.8, line 6 and Figure 3) To summarize, the BIOS of the computer system controls a **master key**, and the firmware update application must have access to this key in order to provide a firmware update to any device in the computer system. (Spec., p.8, lines 3-4)

In contrast to the present invention, the combination of AAPA and Brownell fails to teach or suggest determining whether the firmware update application has access to a **predetermined encryption key utilized by the computer system**. The Examiner acknowledges that AAPA fails to teach or suggest verifying that a firmware update application has the authority to perform activity (such as a firmware update). As such, AAPA fails to teach

or suggest that this step of verifying comprises the step of determining, as noted above. Brownell fails to remedy the deficiencies of AAPA. The Examiner points to Brownell as disclosing the step of determining whether an application has access to a predetermined encryption key. (Office Action, p.4) However, the cited portions of Brownell fail to teach or suggest determining whether the firmware update application has access to a predetermined encryption key **utilized** by **the computer system**. Brownell, at best, teaches that in order to verify the signature of a certificate 122, authorization verifier 147B uses a certificate authority *public key* 141B, which is widely and publicly distributed within the system of intended use such that application 102 and components 104A-B all have access to a copy of this public key. (Brownell, col. 7) That is, in Brownell, the verifier uses a *public key* that is accessible by all applications and components in order to verify a certificate. This is in direct contrast to the system and methods of the present invention, in which a determination is made as to whether the encryption key that the firmware update application has access to is, indeed, the same (private) key that the computer system (such as the BIOS) has access to. Unlike in Brownell, it is not always the case that the key will be the same between the BIOS and the firmware update application, and thus, verifying that the firmware update application has access to this same key as the computer system provides verifying information.

Additionally, while the Examiner has pointed to Freeman as disclosing that a predetermined encryption key is maintained by a BIOS of the computer system (Office Action, p.6), Applicants submit that Freeman also fails to teach or suggest this limitation. Specifically, the cited portions of Freeman discuss the use of a Manufacture Server Public Key that is encrypted with a manufactured computer's BIOS private key. The client computer receives a packet encrypted with the Server Public Key Encrypted with BIOS Private Key portion and uses

a stored and decrypted Server Public Key portion to decrypt the encrypted request packet, comparing the NONCE (i.e., timestamp) to determine if the packet is authentic. (Freeman, [0021]-[0026]) Again, the verification step does not determine if a firmware update application (to which the Examiner equates the client computer) has access to a **predetermined encryption key utilized by the computer system.** Instead, Freeman teaches the use of a Server Public Key to decrypt and verify a packet, but not the step of determining whether the client has access to the BIOS private key. As such, Freeman, taken alone or in combination with AAPA and Brownell, fails to teach or suggest each and every limitation of the independent claims.

For at least these reasons, the combination of AAPA and Brownell, and AAPA, Brownell, and Freeman, fail to teach or suggest each and every element of the independent claims, and as such, a prima facie case of obviousness has not been established with respect to the independent claims.

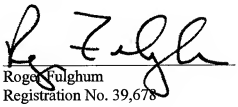
4. Rejection of the Dependent Claims

The dependent claims will not be discussed herein, as these claims depend from otherwise allowable base claims.

Conclusion

Applicants respectfully submit that pending claims 1, 3-9, 11-17, and 19-21 should be passed to issuance.

Respectfully submitted,



Roger Fulghum
Registration No. 39,678

Baker Botts L.L.P.
910 Louisiana
One Shell Plaza
Houston, Texas 77002-4995
(713) 229-1707

Baker Botts Docket Number: 016295.1579

Date: February 26, 2008